

Congress of the United States
Washington, DC 20510

October 31, 2019

The Honorable William P. Barr, Attorney General
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Attorney General Barr,

Child sexual abuse imagery (CSAI) is a plague that companies, government and civil society groups must work together to purge from our society. However, we have serious concerns about the Department of Justice's (DOJ) misguided, hypocritical efforts to pressure technology companies like Facebook into subverting the encryption that protects their messaging apps to enable government access. This proposal will not meaningfully address the problem of CSAI, because illegal content will simply move to the dark web and to foreign commercial providers that are beyond the reach of U.S. law enforcement, while exposing millions of law-abiding Americans to new cybersecurity threats from stalkers, hackers and other criminals.

CSAI is a heinous problem, but it is one that American technology companies have been working to address. As the *New York Times* described in a recent story, the major tech platforms have taken significant voluntary steps to detect and flag CSAI.¹ Last year, tech companies sent 45 million tips to law enforcement. This shocking number highlights not only the enormous nature of the CSAI problem, but also the inadequacy of the government's efforts to date. Quite simply, law enforcement agencies are receiving orders of magnitude more tips than they have the resources to investigate. That must change.

As Members of Congress, we take our responsibility to protect our nation's children seriously. This is why Congress passed the PROTECT Act of 2008 and the Child Protection Act of 2012, both of which require DOJ to take steps to coordinate a cross-sectoral approach to reducing CSAI. Unfortunately, DOJ has failed to comply with parts of these laws, including a requirement that it submit to Congress a National Strategy for Child Exploitation Prevention and Interdiction every two years.² Further, experts have highlighted several immediate steps law enforcement agencies can take to increase their ability to use digital evidence, beyond stopping encryption.³

Rather than focusing the government's resources on reducing the backlog of CSAI reports from tech companies or implementing the reforms required by law and recommended by experts, you have launched a misguided public campaign to pressure Facebook to abandon a cybersecurity upgrade. Facebook announced in January that it intends to upgrade its Instagram and Messenger services with the same form of default encryption that its WhatsApp service has used since 2016. This encryption technology, known as the Signal Protocol, was developed in 2014 by U.S. government-funded researchers, who first included it in Signal, a U.S. government funded app that is popular with cybersecurity experts, policy makers, journalists, and human rights organizations.

Every day, government officials in the White House, DOJ, and Congress use end-to-end encrypted messaging apps like Signal and WhatsApp to protect their unclassified communications. The popularity of these apps among policy makers is not surprising. The Department of Homeland Security revealed last summer that it discovered cell phone spying devices near the White House and other sensitive locations in Washington, D.C.⁴ Likewise, in Senate testimony last year, William Evanina, the top counter-intelligence official in the Office of the Director of National Intelligence, recommended that government officials encrypt their unclassified telephone conversations.⁵

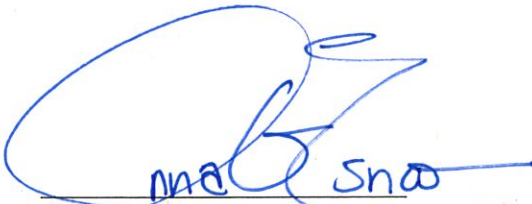
If senior government officials in Washington, D.C. have opted to secure their communications with end-to-end encryption, why should the conversations of millions of law-abiding Americans using Instagram and Facebook Messenger not also be protected from hackers?

The DOJ's public relations campaign to prevent Americans from having the same level of cybersecurity protections as government officials is not just hypocritical, but it has been repeatedly criticized by cryptographers and other leading cybersecurity experts. These technical experts have made it clear that weakening encryption to enable law enforcement access will unnecessarily expose Americans' communications to hacking by criminals and foreign spies. Moreover, if Facebook does bow to your pressure campaign, CSAI predators will simply move to foreign platforms that refuse to cooperate with U.S. law enforcement and are outside of the jurisdiction of our laws and courts. Shifting the problem of CSAI to platforms operated by foreign companies or operating on the dark web would only damage our government's ability to respond to the CSAI epidemic.⁶

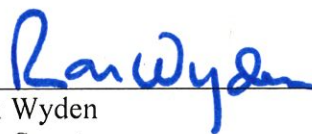
Aside from cybersecurity experts,⁷ the list of people who oppose backdoors includes many former intelligence and military leaders, including Mike McConnell, former Director of the National Security Agency and former Director of National Intelligence; Michael Chertoff, former Homeland Security Secretary; James Baker, former General Counsel of the Federal Bureau of Investigation, William Lynn, former Deputy Defense Secretary; and Michael Hayden, former Director of the National Security Agency and former Director of the Central Intelligence Agency.⁸

We share your concern about CSAI and commit to providing the DOJ with the resources necessary to investigate and prosecute the criminals who create, distribute, and download this material. However, we urge you to stop demanding that private companies purposefully weaken their encryption for the false pretense of protecting children.

Most gratefully,



Anna G. Eshoo
Member of Congress



Ron Wyden
U.S. Senator

-
- ¹ Elie Bursztein et al., “Rethinking the Detection of Child Sexual Abuse Imagery on the Internet,” in WWW ’19 (The World Wide Web Conference, San Francisco, CA, USA, 2019), <https://doi.org/10.1145/3308558.3313482>.
- ² Rep. Debbie Wasserman Schultz, “Letter to Attorney General Barr and Deputy Attorney General Rosen,” August 5, 2019, <https://int.nyt.com/data/documenthelper/1859-wasserman-schultz-letter-doj/7e13eb1633a8a721fa7e/optimized/full.pdf>; Keller and Dance (“Some of the strongest provisions of the law were not fulfilled, and many problems went unfixed, according to interviews and government documents.”).
- ³ William A. Carter and Jennifer C. Daskal, “Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge” (Center for Strategic & International Studies, July 2018), <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>; Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (W. W. Norton & Company, 2018), chap. 9.
- ⁴ Sean Gallagher, “DHS Found Evidence of Cell Phone Spying near White House,” *Ars Technica*, June 1, 2018, <https://arstechnica.com/information-technology/2018/06/dhs-found-evidence-of-cell-phone-spying-near-white-house/>.
- ⁵ “Nomination of William R. Evanina to Be Director of National Counterintelligence and Security Center,” U.S. Senate Select Committee on Intelligence (May 15, 2018), <https://www.intelligence.senate.gov/hearings/open-hearing-nomination-william-r-evanina-be-director-national-counterintelligence-and>.
- ⁶ John DeLong et al., “Don’t Panic: Seeking Points of Agreement on the ‘Going Dark’ Debate” (Berkman Center for Internet & Society at Harvard University’s Berklett Cybersecurity Project, February 1, 2016), <https://cyber.harvard.edu/pubrelease/dont-panic/>.
- ⁷ Harold Abelson et al., “Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications,” *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 69–79, <https://doi.org/10.1093/cybsec/tyv009>; Joseph Marks, “The Cybersecurity 202: Experts Slam Justice’s Move to Make Child Exploitation the Face of Anti-Encryption Push,” *Washington Post*, October 8, 2019, <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/10/08/the-cybersecurity-202-experts-slam-justice-s-move-to-make-child-exploitation-the-face-of-antiencryption-push/5d9b664e88e0fa747e6d5169/>.
- ⁸ Mike McConnell, Michael Chertoff, and William Lynn, “Why the Fear over Ubiquitous Data Encryption Is Overblown,” *Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; Tom Ashbrook, “Michael Hayden: America Is Safer With End-To-End Encryption,” *WBUR’s On Point*, March 1, 2016, <https://www.wbur.org/onpoint/2016/03/01/michael-hayden-nsa-encryption>.